

Approved:

  
JERRY J. FANG  
Assistant United States Attorney

Before: THE HONORABLE GABRIEL W. GORENSTEIN  
United States Magistrate Judge  
Southern District of New York

**23 MAG 1796**

-----X	:	
UNITED STATES OF AMERICA	:	<b><u>SEALED COMPLAINT</u></b>
	:	
- v. -	:	Violations of 18 U.S.C. §§ 371,
	:	1349, 2315, and 2.
	:	
OLUSEUN MARTINS OMOLE,	:	COUNTY OF OFFENSE:
a/k/a "Seun Omole,"	:	NEW YORK
	:	
Defendant.	:	
	:	
-----X	:	

SOUTHERN DISTRICT OF NEW YORK, ss.:

MARY BOOTHE, being duly sworn, deposes and says that she is a Special Agent with the Federal Bureau of Investigation ("FBI") and charges as follows:

**COUNT ONE**

(Conspiracy to Commit Wire Fraud)

1. From at least in or about September 2019 through at least in or about November 2022, in the Southern District of New York and elsewhere, OLUSEUN MARTINS OMOLE, a/k/a "Seun Omole," the defendant, and others known and unknown, willfully and knowingly combined, conspired, confederated, and agreed together and with each other to commit wire fraud, in violation of Title 18, United States Code, Section 1343.

2. It was a part and object of the conspiracy that OLUSEUN MARTINS OMOLE, a/k/a "Seun Omole," and others known and unknown, knowingly having devised and intending to devise a scheme and artifice to defraud, and for obtaining money and property by means of false and fraudulent pretenses, representations, and promises, would and did transmit and cause to be transmitted by means of wire, radio, and television communication in interstate and foreign commerce, writings, signs, signals, pictures, and sounds for the purpose of executing such scheme and artifice, in violation of Title 18, United States Code, Section 1343, to wit, OMOLE participated in a scheme that involved, among other things, the use of false pretenses communicated by email and text message to fraudulently induce victims to ship packages containing electronic devices to OMOLE, which he then reshipped to co-conspirators located

outside of the United States.

(Title 18, United States Code, Section 1349.)

**COUNT TWO**

(Conspiracy to Commit Receipt of Stolen Goods  
and Interstate and Foreign Transportation of Stolen Goods)

3. From at least in or about September 2019 through at least in or about November 2022, in the Southern District of New York and elsewhere, OLUSEUN MARTINS OMOLE, a/k/a “Seun Omole,” the defendant, and others known and unknown, willfully and knowingly did combine, conspire, confederate, and agree together and with each other to commit an offense against the United States, to wit, interstate and foreign transportation of stolen goods, in violation of Title 18, United States Code, Section 2314, and receipt of stolen goods, in violation of Title 18, United States Code, Section 2315.

4. It was a part and object of the conspiracy that OLUSEUN MARTINS OMOLE, a/k/a “Seun Omole,” the defendant, and others known and unknown, knowingly transported, transmitted, and transferred in interstate and foreign commerce goods, wares, merchandise, securities, and money, of the value of \$5,000 and more, knowing the same to have been stolen, converted, and taken by fraud, in violation of Title 18, United States Code, Section 2314.

5. It was a further part and object of the conspiracy that OLUSEUN MARTINS OMOLE, a/k/a “Seun Omole,” the defendant, and others known and unknown, knowingly received, possessed, concealed, stored, bartered, sold, and disposed of goods, wares, merchandise, securities, and money of the value of \$5,000 and more, and pledged or accepted as a security for a loan any goods, wares, merchandise, and securities, of the value of \$500 and more, which had crossed a State and United States boundary after being stolen, unlawfully converted, and taken, knowing the same to have been stolen, unlawfully converted, and taken, in violation of Title 18, United States Code, Section 2315.

**Overt Acts**

6. In furtherance of the conspiracy and to effect the illegal objects thereof, the following overt acts, among others, were committed in the Southern District of New York and elsewhere:

a. In or about February 2021, an individual representing himself to be “Tobylink Fadaca” fraudulently induced a victim residing in the Southern District of New York to send a smartwatch to a location in Texas controlled by OLUSEUN MARTINS OMOLE, a/k/a “Seun Omole,” the defendant, who had incorporated a business entity named Tobylink Impressions, a/k/a Tobylink Impressions, for use in the Fraud Scheme.

(Title 18, United States Code, Section 371.)

**COUNT THREE**

(Receipt of Stolen Goods)

7. From at least in or about September 2019 through at least in or about November 2022, in the Southern District of New York and elsewhere, OLUSEUN MARTINS OMOLE, a/k/a “Seun Omole,” the defendant, knowingly received, possessed, concealed, stored, bartered, sold, and disposed of goods, wares, merchandise, securities, and money of the value of \$5,000 and more, and pledged or accepted as a security for a loan any goods, wares, merchandise, and securities, of the value of \$500 and more, which had crossed a State and United States boundary after being stolen, unlawfully converted, and taken, knowing the same to have been stolen, unlawfully converted, and taken, to wit, OMOLE received in Texas at least approximately 5,900 packages from victims of various scams and confidence tricks residing throughout the United States, including victims residing in Manhattan, New York.

(Title 18, United States Code, Sections 2315 and 2.)

The bases for my knowledge and the foregoing charges are, in part, as follows:

8. I am a Special Agent with the FBI. I have been personally involved in the investigation of this matter, and I base this affidavit on that experience, on my conversations with other law enforcement agents, witnesses, and others, and on my examination of various reports and records. Because this affidavit is being submitted for the limited purpose of demonstrating probable cause, it does not include all the facts that I have learned during the course of my investigation. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

**Overview of the Fraud Scheme**

9. I am personally involved in an ongoing investigation being conducted by the FBI into a nationwide fraud scheme in which perpetrators of the scheme obtain money or property from victims using a variety of different fraudulent scams and direct the victims to send money or property to co-conspirators, who in turn repackage the property and send the property overseas to the lead perpetrators of the scheme (the “Fraud Scheme”).

10. One of the types of scams employed by the perpetrators of the fraud scheme is a romance scam, which is a confidence trick that involves a co-conspirator feigning romantic intentions toward a victim, gaining their trust and affection, and then taking advantage of that goodwill to commit fraud, for example, by inducing the victim to send money or property to the perpetrator based on false or fraudulent pretenses.

11. Another scam employed by the perpetrators of the fraud is an online marketplace scam. In such a scam, the perpetrators of the scam may contact a victim who is selling an item on an online marketplace to purchase that item. The perpetrators may then send fraudulent communications to the victim of the scam, purportedly as the online marketplace, falsely advising

the victim that the item was sold and that the payment to the victim was completed, and instructing the victim to send the item to the participants in the scheme, even though, in fact, no payment had been received by the victim.

12. Further, the perpetrators of the fraud scheme used employment scams to fraudulently obtain money or property. Such a scam involves a fraudulent job posting, such as for a remote, entry-level position, which may be posted by the perpetrators of the fraud online. After informing victims of the scam that they were hired, the perpetrators of the fraud may then direct the victims to send property to the participants in the scheme, but without compensating the victims.

#### OLUSEUN MARTINS OMOLE's Participation in the Fraud Scheme

13. Based on my discussions with other law enforcement officers, I have learned that OLUSEUN MARTINS OMOLE a/k/a "Seun Omole," the defendant, is a Nigerian national who entered the United States on a visa and has overstayed his visa since 2017.

14. Based on my participation in this investigation and my review of open-source information, I know that OLUSEUN MARTINS OMOLE, a/k/a "Seun Omole," the defendant, is the owner, director, and purported chief executive officer ("CEO") of a domestic business corporation named Tobylink Impessions, Inc. a/k/a Tobylink Impressions Inc. ("Tobylink"). Specifically, based on my review of Delaware and Texas Secretary of State records, I know that Tobylink was incorporated in 2002 in the State of Delaware and registered for tax obligations in 2021 in the State of Texas, with OMOLE listed as director. In addition, my review of a LinkedIn profile for an individual by the name of "Seun Omole" reflects that this individual listed himself as the CEO of Tobylink. Based on my comparison of this LinkedIn profile with a Facebook profile for an individual by the name of "Oluseun Omole," who lists himself as employed at Tobylink, I believe OMOLE to be the owner of both accounts based on consistent listed educational history, among other things.

15. Based on my review of Tobylink's publicly available website (*i.e.*, tobylink.com), I have learned that Tobylink bills itself as a "world leading Procurement, Distributor, Reseller and trusted supplier of VSAT Satellite Communications Equipment, Electrical and Electronics wire & cable." According to its website, Tobylink purports to serve as a business-to-business vendor of specialized equipment and service solutions, as opposed to dealing in consumer or retail goods.

16. Based on my review of publicly available social media profiles, I have also learned that Tobylink maintains an Instagram account with the handle @tobylinkimp, which appears to list Tobylink's services as "International Freight & Logistics." Based on my training and experience, I believe that this Instagram account belongs to Tobylink because (i) the logo in the profile picture of the Instagram account matches the logo depicted on Tobylink's website; (ii) the Instagram account with the handle @tobylinkimp contains a link to Tobylink's website; and (iii) a post on the Instagram account contains a phone number that is the same phone number listed on OMOLE's business card and Tobylink's website.

17. Despite Tobylink's public-facing representations on its website and Instagram page as to the nature of its business, Tobylink does not appear to be a bona fide procurer, distributor, reseller, or supplier of satellite communications equipment, based on my review of export records provided by CBP. Rather, there is probable cause to believe that Tobylink's primary purpose was to further the Fraud Scheme by enabling OLUSEUN MARTINS OMOLE, a/k/a "Seun Omole," the defendant, to receive fraudulently obtained consumer goods, re-package those goods, and then ship them to co-conspirators in Nigeria. Specifically, based on my participation in the investigation, conversations with other law enforcement officers, and my review of records and reports, I have learned the following, in substance and in part:

a. From in or about January 2020 through in or about November 2022, Tobylink received approximately 5,900 packages from three private mail carriers ("Carrier-1," "Carrier-2," "Carrier-3") and the United States Postal Service, initially, at a storage unit located in Richmond, Texas (the "Storage Unit"), and at a warehouse located in Richmond, Texas (the "Warehouse") after Tobylink was evicted from the Storage Unit, as discussed in paragraph 18, *infra*.

b. These packages, which typically contained high-value personal property such as smartphones, computers, tablets, and smartwatches, were sent by victims of the Fraud Scheme to OMOLE at the Storage Unit or the Warehouse, often at the direction of OMOLE's co-conspirators. In total, OMOLE received at least an estimated \$4,720,000 in fraudulently obtained consumer goods.<sup>1</sup>

18. Based on my participation in the investigation, conversations with other law enforcement officers and employees of the storage company that leased the Storage Unit ("Company-1") to OLUSEUN MARTINS OMOLE, a/k/a "Seun Omole," the defendant, and my review of records, reports, and open-source information, I have learned the following, in substance and in part:

a. OMOLE informed a former employee of Company-1 who was employed by Company-1 between 2019 and November 2020 ("Employee-1") that Tobylink shipped packages overseas. Employee-1 also observed OMOLE consistently receiving a large number of packages at the Storage Unit, and possibly hundreds each month. In addition, Employee-1 received phone calls from individuals who had sent packages to Tobylink complaining about being defrauded by Tobylink.

b. A former interim manager of Company-1 between in or about

---

<sup>1</sup> Based on my training and experience investigating similar re-shipping fraud schemes, it is probable that the vast majority of the packages received by Tobylink were obtained as a part of the Fraud Scheme based on the fact that Tobylink does not appear to have any legitimate business operations. For such extensive fraud schemes, it is also typical to approximate the dollar amount of the fraud—here, by multiplying the number of packages received by Tobylink by \$800, which is a reasonable estimate for the retail price of a new smartphone. This estimate is conservative, however, because the retail price of a laptop or tablet may exceed \$800 in many circumstances.

May 2021 through in or about July 2021 (“Manager-1”) also observed OMOLE receiving over ten packages daily, and in some instances, as many as twenty or nearly thirty. Manager-1 and another former interim manager who worked for Company-1 during the same timeframe (“Manager-2”) also received constant phone calls from individuals claiming that Tobylink had their stolen items and that they were victims of fraud by Tobylink.

c. During this time, Manager-1, Manager-2, and the soon-to-be manager of Company-1 starting in July 2021 (“Manager-3”) also observed members of law enforcement on Company-1’s premises, looking for individuals associated with Tobylink based on reports of fraud being conducted by Tobylink, as well as goods that were shipped to Tobylink that had been reported stolen to law enforcement.

d. Eventually, at the direction of Company-1’s corporate parent, Company-1’s management stopped accepting packages for Tobylink and the Storage Unit, and employees of Company-1 were instructed not to sign for any packages relating to Tobylink. OMOLE confronted Manager-2, with Manager-3 also present, asking Manager-2 why Company-1 was stopping his packages from being received. Manager-2 informed OMOLE that Company-1 was receiving phone calls from individuals claiming that the packages shipped to Tobylink contained stolen items. OMOLE denied any involvement in stealing items, claiming that he merely provided third party shipping services for clients who sent him items to ship overseas.

e. Despite Company-1’s efforts to cease accepting packages for Tobylink, OMOLE continued to receive packages at the Storage Unit by simply receiving them directly from mail carriers. OMOLE was evicted from the Storage Unit in or about July 2021. Even after OMOLE’s eviction, Manager-3 received phone calls from individuals who sent packages to Tobylink claiming to have been defrauded.

19. I have also participated in interviewing numerous victims of the Fraud Scheme,<sup>2</sup> which establish that the involvement OLUSEUN MARTINS OMOLE, a/k/a “Seun Omole,” the defendant, in the Fraud Scheme began at least as early as in or about September 2019.

#### Victim-1

20. In or about August 2022, I interviewed a victim of a romance scam in connection with the Fraud Scheme (“Victim-1”). Based on my interview of Victim-1, who resides in Oregon, and my review of materials provided by Victim-1, I have learned the following, in substance and in part:

a. In or about June 2019, Victim-1 met an individual who used the fake name Simon Howard (“Howard”) on a dating application. Victim-1 believed that Howard resided in Portland, Oregon, which she later learned to be false. After messaging with the person posing as Howard on the dating application, Victim-1 then proceeded to exchange text messages with that person, as well as on a third-party messaging application.

---

<sup>2</sup> The examples set forth in this Complaint are not intended to represent an exhaustive list of victims of the Fraud Scheme.

b. The person posing as Howard told Victim-1 a series of lies to gain her trust. The person posing as Howard informed Victim-1 that he worked for the World Health Organization and that he was in Ukraine for a construction project, but that he had purchased a house in Portland, Oregon. However, according to the person posing as Howard, the house was going into escrow earlier than anticipated, and thus, he was unable to pay certain fees associated with the construction project. The person posing as Howard preyed on Victim-1's religious convictions, telling her that he owed approximately \$28,000 and suggesting that Victim-1 pray about what she should do.

c. In or about July 2019, Victim-1 agreed to help the person she believed to be Howard pay the purported fees using a combination of money she had in her bank account, her credit card, potential bank loans, and her retirement funds. As Victim-1's online relationship with the person she believed to be Howard continued, Victim-1 sent him thousands of dollars in Bitcoin and gift cards and through wire transactions. Victim-1 also gave COVID-19 pandemic relief funds she received to that person.

d. In addition, Victim-1 also purchased consumer electronics for the person she believed to be Howard, including at least two Apple Macbook Pro laptops, two Apple Macbook Air laptops, two Apple smartphones, two Apple Watches, and two Apple AirPods. At the direction of the person posing as Howard, Victim-1 sent some of the consumer electronics through Carrier-2 in at least three shipments between in or about September 2019 and in or about October 2019 to Tobylink at the address associated with the Storage Unit. Victim-1 also sent other consumer electronics to other participants of the Fraud Scheme in New York, New York.

e. In or about November 2019, Victim-1 confronted the person posing as Howard, who had purportedly received \$625,000 from the sale of a house and claimed to have sent Victim-1 a check for \$285,000. Victim-1 did not receive the purported check for \$285,000, or any repayment for the funds she sent to that person or any payment for the consumer electronics that she sent to Tobylink.

### Victim-2

21. In or about January 2022, I interviewed another victim of a romance scam in connection with the Fraud Scheme ("Victim-2"). Based on my interview of Victim-2, who resides in California, and my review of materials provided by Victim-2, I have learned the following, in substance and in part:

a. In or about November 2019, Victim-2—whose husband had passed away approximately twenty years ago—met an individual on a social media website who falsely introduced himself as a five-star general in the United States military with the fake name "Scott Rolland," and later also identified himself as "Rolland Cadwell Allyn Scott."<sup>3</sup> The person posing

---

<sup>3</sup> Based on open-source research, for example, I have learned that no military officers have held a five-star rank since in or about 1981.

as Rolland told Victim-2 falsehoods that he was shot while on patrol in Afghanistan, that he needed surgery, and that he was struggling with medical payments despite receiving a 50% military discount.

b. Around this time, Victim-2 began sending money to the person she believed to be Rolland. Eventually, Victim-2 and the person posing as Rolland moved their conversations onto another messaging application, and as their relationship continued to develop, the person she believed to be Rolland began to ask for additional financial assistance and favors. For example, he falsely represented that he had a bank account in the United States, but because he was abroad, there were restrictions on his account. Thus, the person posing as Rolland asked Victim-2 to send money to a friend on that person's behalf, which Victim-2 sent in Bitcoin.

c. In addition, the person posing as Rolland told Victim-2 that while he was a part of an Army Ranger unit, his team found \$25 million in Afghanistan that he was in charge of distributing, and that he needed money to extract the \$25 million from Afghanistan and to send his \$2.5 million cut to his daughter in Florida—none of which was actually true.<sup>4</sup> Victim-2 agreed to send who she believed to be Rolland money in the form of cashier's checks to a co-conspirator, who would then send the money to Rolland. Although the person posing as Rolland informed Victim-2 that he was working with the embassy to reimburse her and that he wanted to give Victim-2 access to his bank account to show that he had the money to repay her, Victim-2 did not receive any repayments.

d. In or about August 2020, at the direction of the person posing as Rolland, Victim-2 also sent at least five smartphones through Carrier-1 to Tobylink at the address associated with the Storage Unit.

e. In or about March 2021, Victim-2 started to become suspicious and began researching "General Allyn." After determining that she was speaking with an impostor and that there did appear to be a real, retired U.S. Army general with a surname of "Allyn," Victim-2 drafted a letter to General Allyn to inform him that someone had been impersonating him. In or about July 2021, Victim-2 sent the letter to an email address she believed to belong to General Allyn, but was actually controlled by a member of the Fraud Scheme. The recipient of the email, posing as General Allyn, responded with feigned concern and requested that Victim-2 send him \$5,000 to research the matter further. Victim-2 sent the person she believed to be General Allyn the money from her savings.

f. The person posing as General Allyn sent pictures to Victim-2, purportedly of the FBI arresting the individuals to whom Victim-2 sent money. He also informed Victim-2 that Rolland—the fictitious individual with whom Victim-2 had entered into a relationship—was located in Nigeria and requested additional money to arrest Rolland, at which point Victim-2 realized that she had been defrauded again.

---

<sup>4</sup> To further gain Victim-2's trust, the person posing as Rolland also introduced Victim-2 to his purported daughter, who does not appear to exist. Victim-2 developed an online relationship with Rolland's "daughter," eventually asking Rolland to allow her to be the custodian for his purported daughter. Rolland also proposed to Victim-2, who agreed to marry him.

g. In sum, Victim-2 sent hundreds of thousands of dollars to the participants of the Fraud Scheme. The funds included those set aside for Victim-2's children, a \$200,000 loan that Victim-2 took out on her house, money from Victim-2's investment accounts, as well as the proceeds from the sale of Victim-2's business.

#### Victim-3

22. In or about August 2022, I interviewed a victim of an online marketplace scam in connection with the Fraud Scheme ("Victim-3"). Based on my interview of Victim-3, who resides in Watertown, New York, and my review of materials provided by Victim-3, I have learned the following, in substance and in part:

a. In or about December 2020, Victim-3 listed a Microsoft Surface Pro for sale on an online auction website. After a purported buyer entered a bid to buy the computer for \$600, Victim-3 accepted the offer. Victim-3 received an email on his email address, purportedly from the online auction website, indicating that the online auction website had received a payment from the putative buyer and that the funds were being held by an online payment service ("Online Payment Service-1") until Victim-3 provided the tracking number for shipping the computer to the putative buyer, after which Victim-3 would receive the payment.

b. As instructed by the supposed buyer, Victim-3 sent the computer to Tobylink at the address associated with the Storage Unit through the United States Postal Service and provided the tracking number to the email account he believed to be associated with the online auction website. The email address purportedly associated with the online auction website confirmed the receipt of the tracking number and promised to process the payment after verifying that the shipment had been received. However, Victim-3 never heard from the purported online auction website, nor did he actually receive any payment for the computer from the supposed buyer or Online Payment Service-1.

c. Victim-3 called an actual number for the online auction website to request an update on the status of his payment, but the online auction website informed Victim-3 that they had no record of any payments being made or any emails sent by the real online auction website. The online auction website also advised that they did not communicate with sellers on their personal email addresses.

#### Victim-4

23. In or about August 2022, I interviewed another victim of an online marketplace scam in connection with the Fraud Scheme ("Victim-4"). Based on my interview of Victim-4, who resides in Middletown, New York, and my review of materials provided by Victim-4, I have learned the following, in substance and in part:

a. In or about February 2021, Victim-4 listed his Apple Watch and charger for sale on an online marketplace. A buyer, purporting to be someone by the name of "Tobylink Fadaca," contacted Victim-3 by text message, offering to purchase the Apple Watch and

charger for \$500 through an online payment service (“Online Payment Service-2”).

b. The person purporting to be Tobylink Fadaca falsely informed Victim-4 that the money had been sent to Victim-4 through Online Payment Service-2, after which Victim-4 received an email purporting to be from Online Payment Service-2. The email also represented that the purported buyer’s money would be held until the tracking number for the shipment was entered.

c. Victim-4 used Carrier-1 to ship the Apple Watch and charger from Middletown, New York, to Tobylink Fadaca at the address of the Storage Unit in Richmond, Texas. Subsequently, Victim-4 responded with the tracking number to the email that he had received, supposedly from Online Payment Service-1, in order to release the buyer’s money.

d. However, Victim-4 never received the money from Tobylink Fadaca for his Apple Watch and charger. Instead, Victim-4 received an email from the same email account pretending to be Online Payment Service-1, falsely stating that while the shipment tracking number had been received, there were technical issues with Victim-4’s account that prevented the \$500 from being credited. Victim-4 received another email from the pretend Online Payment Service-1 email account that he received an additional \$700 from Tobylink Fadaca, that his account had been upgraded to a business account, and that he would need to send \$700 to Tobylink Fadaca using another online payment service (“Online Payment Service-3”) and proof that the \$700 had been sent as directed in order for the \$1,200 held by Online Payment Service-2 to be released to Victim-4’s account.

e. Victim-4 had not actually created any business account with Online Payment Service-2. After receiving the email, purportedly from Online Payment Service-2, instructing Victim-4 to send another \$700 to the buyer, Victim-4 contacted the email account he believed to be Online Payment Service-2, indicating that he did not have the necessary funds and requesting assistance with having his Apple Watch returned.

f. Victim-4 also contacted the person purporting to be Tobylink Fadaca to return his Apple Watch, but was informed that while Tobylink Fadaca had received the watch, he claimed that he could not return the watch because he lacked the funds to ship the watch back to Victim-4. The person purporting to be Tobylink Fadaca indicated that he was willing to return the watch, but only if Victim-4 sent additional money to cover overnight shipping to an account with Online Payment Service-2 that was associated with someone Tobylink Fadaca identified to be his purported sister.

g. In or about March 2021, Victim-4 contacted the email account that he believed to be associated with Online Payment Service-2, advising that he had tried, but was unable, to send the funds to cover overnight shipping, as directed by the person Victim-4 believed to be Tobylink Fadaca. The purported Online Payment Service-2 account falsely informed Victim-4 that there were issues with his account, asking for Victim-4’s online access and PIN with Online Payment Service-2, along with Victim-4’s Social Security Number. Victim-4 provided his PIN and continued to correspond with the purported Online Payment Service-2 email address regarding issues with his account. The purported Online Payment Service-2 email address also asked for

Victim-4's contact information associated with his account, as well as pictures of the front and back of his debit card and the associated zip code. Victim-4 provided the phone number linked to his actual account with Online Payment Service-2, but declined to provide the rest of the requested information. Victim-4 never received any payment for the Apple Watch.

Victim-5

24. In or about August 2022, I interviewed a victim of an employment scam in connection with the Fraud Scheme ("Victim-5"). Based on my interview of Victim-5, who resides in Alaska, and my review of materials provided by Victim-5, I have learned the following, in substance and in part:

a. In or about December 2021, Victim-5 responded to a job advertisement for a remote work position with a company purportedly named "Continuum Global Solutions," which was posted on a social media website. After messaging with the listed job contact regarding the contours of the purported position, Victim-5 was instructed to download another text messaging application to conduct an interview with someone named "Harry Applegate," who claimed to be the company's hiring agent.

b. After interviewing with the individual posing as Applegate by text message, Victim-5 received the purported position and received further instructions from the individual posing as Applegate as to the training and orientation process. The person posing as Applegate represented, among other things, that Victim-5 would need to add a new phone line to her existing phone plan for the iPhone that she would be using for the purported job. The person posing as Applegate also informed Victim-5 that she would need to purchase a new iPhone, and that the phone would need to be shipped to the company's purported vendor to install unspecified software on the phone.

c. The person posing as Applegate instructed Victim-5 to ship the smartphone overnight through Carrier-1 to "Tobylink Fadaca" at the address associated with the Storage Unit, promising that after the purported software installation, Tobylink Fadaca would send the phone back to Victim-5 to start training for the purported job.

d. After confirming that Tobylink Fadaca had received the phone, the person posing as Applegate also requested that Victim-5 purchase a credit card to set up an online portal to track the hours that Victim-5 would work for the purported job, and for the purported installation of software on the smartphone and laptop that Victim-5 would be using for the purported job.

e. Victim-5 became suspicious and asked the person she believed to be Applegate to return the phone that she had shipped to Tobylink Fadaca. The person posing as Applegate never responded, and instead proceeded to delete the text exchange that he had with Victim-5. Victim-5 never received any payment for the phone, nor was the phone that Victim-5 sent to Tobylink Fadaca returned to Victim-5.

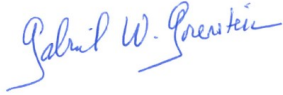
WHEREFORE, I respectfully request that a warrant be issued for the arrest of OLUSEUN MARTINS OMOLE, a/k/a "Seun Omole," the defendant, and that he be arrested, and imprisoned or bailed, as the case may be.

/s/ sworn telephonically

---

MARY BOOTHE  
Special Agent  
Federal Bureau of Investigation

Sworn to me through the transmission of this Complaint  
by reliable electronic means, pursuant to Federal Rules of  
Criminal Procedure 41(d)(3) and 4.1, this 6 day of March, 2023



---

THE HONORABLE GABRIEL W. GORENSTEIN  
UNITED STATES MAGISTRATE JUDGE  
SOUTHERN DISTRICT OF NEW YORK